CITY OF HOUSTON

Executive Order

Subject: **Information Technology Security**	E.O. No: **1-48**
	Effective Date: **July 9, 2013**

1. AUTHORITY

1.1 Article VI, Section 7a, City Charter of the City of Houston.

2. PURPOSE

2.1 To provide consistent policies regarding information technology (IT) security and the roles and responsibilities of personnel using and maintaining computer resources, electronic communications and internet access in performance of their job function

3. OBJECTIVES

3.1 Protect all City of Houston information and information systems in a manner that is commensurate with the security classification level, sensitivity, value, and critical nature of Information.

3.2 Protect information from unauthorized access, disclosure, destruction, disruption, or modification while the information is being collected, processed, transmitted, stored, or disseminated.

3.3 Manage all information technology that is acquired, developed, or used in support of City programs, projects, and department requirements by use of a process that covers the complete system lifecycle.

3.4 Manage all information systems in a cost-effective manner, guided by the application of sound risk management processes that ensure an appropriate level of integrity, confidentiality, and availability of information in each phase of the system lifecycle.

3.5 Conduct periodic audits of all City information systems that process, store, or transmit City data.

3.6 Investigate information security incidents for incident management, forensic investigations, and reports.

3.7 Ensure all basic information security policy requirements, audits, and forensic investigations are implemented across all City departments and activities.

4. DEFINITIONS

Information – Any knowledge that can be communicated regardless of physical form or characteristic; which is owned by, produced by, produced for, or is under the control of the City of Houston.

Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide confidentiality, integrity, and availability.

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment is used in the automation acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the City of Houston. This includes computers, laptops, wireless air-cards, electronic mobile devices, ancillary equipment, software, firmware, and similar procedures, services (including support services), including but not limited to credit card and online payment processing systems and services, telecommunications systems and related resources.

5. SCOPE

5.1 This executive order is applicable to all City offices and departments. This executive order also applies to City contractors and City grantees, to the extent specified in their contract, grant, or agreement. City employees shall abide by the requirements of this executive order when they are using City resources or performing City duties.

5.2 Facilities, resources, and personnel under a contract or grant from the City at a college, university, or research establishment are included in the applicability of this executive order.

6. RESPONSIBILITIES

6.1 The Mayor hereby delegates to the Chief Information Officer (CIO) and Department Directors the authority to ensure compliance with the requirements contained in this executive order.

6.2 The CIO shall:

6.2.1 Develop and maintain a City-wide information security program. This shall be accomplished by establishing and implementing information security and information system security policies and issuing instructions, memoranda, and bulletins designed to facilitate appropriate protection and accountability of information.

6.2.2 Designate a Chief Information Security Officer (CISO).

6.2.3 Ensure that information security management processes are integrated with the City's strategic and operational processes and are compliant with local, state and federal laws, and Payment Card Industry Data Security Standards.

6.2.4 Ensure the development and maintenance of information security policies and procedures to protect information.

6.2.5 Ensure the development and maintenance of a security certification program for security authorization of City information systems.

6.2.6 Develop and maintain information security procedures and control techniques to address all applicable requirements of the City information security program.

6.2.7 Train and oversee personnel with responsibilities for information security with respect to such responsibilities.

6.2.8 Issue procedural requirements updates regarding protection and management of information and IT resources in the form of a City Information Technology Requirement (CITR), as necessary, to keep pace with the dynamic information security environment.

6.2.9 Charter a City Security Operations Center (SOC) that provides consolidated information security operations and incident response capability that provides City-wide visibility and monitoring of City networks and systems.

6.2.10 Ensure procedures are established for referral of suspected and confirmed computer crimes involving information systems to law enforcement and other agencies, as appropriate, for investigation in a timely manner. Computer crimes include:

6.2.10.1 Unauthorized access of information.

6.2.10.2 Compromises of computers, laptops, wireless air-cards, electronic mobile devices and ancillary equipment.

6.2.10.3 Compromises of IT resources such as telecommunications systems, command and control systems, and network systems.

6.2.11 Coordinate the initial assessment of suspected computer crimes related to information or information systems, such as unauthorized access of information, compromises of computers, laptops, wireless air-cards, electronic mobile devices, ancillary equipment and other IT resources, such as telecommunications systems, command and control systems, and network systems, with law enforcement and other agencies, as appropriate.

6.2.12 Establish a City-wide information security capability for information and information systems with the mission and resources to:

6.2.12.1 Develop and implement an information security review program designed to ensure that all City information systems used to process information are in compliance with City policy, City procedural requirements, and any applicable federal and state guidelines and statutes. Information security reviews shall be coordinated with City departments to ensure that the review efforts are not duplicated.

6.2.12.2 Investigate Information Security incidents.

6.2.13 Charter a City Information Technology Security Advisory Group (ITSAG) to advise the IT Governance Board, the CISO, and the City departments on information security issues.

6.3 The CISO shall:

6.3.1 Carry out the CIO's responsibility for information security.

6.3.2 Carry out the CISO responsibilities described in E.O. 1-44, Information Technology Governance.

6.3.3 Possess professional qualifications, including training and experience, required to administer the functions described under this section.

6.3.4 Be responsible for information security duties.

6.3.5 Establish an office with the mission and resources for information security operations, security governance, security architecture and engineering, and cyber-threat analysis to assist in ensuring City-wide compliance with City security policies and procedures.

6.3.6 Provide management and oversight of the City SOC.

6.3.7 Manage the City's information security program and activities for information and information systems; including the preparation and maintenance of enterprise security policies, procedures, and processes.

6.3.8 Serve as the liaison between the City Attorney, the City SOC, and the Department Directors to ensure City-wide uniformity from the legal perspective and with respect to identifying and complying with the applicable laws relating to Information Security.

6.3.9 Provide program management of the City's information security programs and projects.

6.3.10 Serve as the City Information System Risk Executive, responsible for ensuring that security risk-related considerations and risk management of individual information systems are consistent across the City, are reviewed from a City-wide and strategic goal perspective, and reflect the City's information system risk tolerance affecting mission/business success.

6.3.11 Establish and manage the City information security performance metrics program.

6.4 The Department Directors shall:

6.4.1 Have the responsibility to provide information security for the information systems that support the operations and assets under their control by:

6.4.1.1 Assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

6.4.1.2 Determining the levels of information security appropriate to protect such information and information systems for information security classifications and related requirements.

6.4.1.3 Implementing policies and procedures to cost-effectively reduce risks to an acceptable level.

6.4.1.4 Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

6.4.1.5 Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

6.4.2 Designate a department Information Security Officer (ISO) (shared in the case of smaller departments) who shall:

6.4.2.1 Assist the Department CTOs (Chief Technology Officers), Assistant Directors of IT, and Deputy CIOs, in implementing this policy and other City information security policies and procedures, and any applicable federal and state information security laws, directives, policies, standards, and guidelines.

6.4.2.2 Confer with the City Attorney to address potential and actual legal issues involving Information Security.

6.4.2.3 Participate as the Department's representative to the City ITSAG.

6.4.3 Support the Department CTOs, Assistant Directors of IT, and Deputy CIOs, in acquiring adequate staff, resources, budget, and authority to implement the information security programs and projects within the purview of the Department.

HITS shall provide services to departments that do not maintain the staff to support an internal IT infrastructure, including but not limited to a Department CTO or other executive IT personnel. HITS shall proactively advise, provide risk assessments and support these departments as needed.

6.5 If designated by the department director, the Department CTOs, Assistant Directors of IT, and Deputy CIOs for information and information systems under their purview shall:

6.5.1 Be responsible and accountable for the protection of the information and the IT resources under their cognizance.

6.5.2 Be responsible and accountable for compliance with this policy, other City information security policies and procedures and any applicable Federal and State information security laws, directives, policies, standards, and guidelines.

6.5.3 Be responsible for the Department's mission and resources for information security operations, security governance, and security architecture and engineering to assist the department director in the compliance with this policy and other City information security policies and procedures.

6.5.4 Be the primary Department interface to the CISO for IT security matters.

6.5.5 Be responsible for the coordination of investigations of information security incidents with the CISO. Referral of an information security incident to an investigating authority shall be made in consultation with the CISO and affected department CTOs.

6.5.6 Make available, qualified personnel to support periodic security assessments conducted by the CISO.

7. CONFLICT AND REPEAL

7.1 This Executive Order supersedes Executive Order 1-48, Policy on Information Technology Security, signed November 3, 2003, which shall be of no further force or effect.